USGS
science for a changing world

Geospatial Digital Rights Management

By Daniel J. Wright

Open-File Report 2005-1086

U.S. Department of the Interior
U.S. Geological Survey

Geospatial Digital Rights Management

Daniel J. Wright
U.S. Geological Survey
511 National Center
Reston, VA 20192

Daniel J. Wright is a student working with the Cooperative Topographic Mapping Program for the U.S. Geological Survey. He will begin his freshman year at the University of North Carolina – Chapel Hill in the Fall of 2005.

Abstract

Distributors of geospatial data must ensure that agreements made with data providers are adhered to by controlling the access and use of data. Digital Rights Management is a way to ensure that these agreements are honored. Digital Rights Management systems include a framework for implementation and rights policies which are attached to data and describe the rights users have regarding the data. Rights policies are written in rights expression languages, one of which, Open Digital Rights Language, is particularly well suited for digital rights management systems for geospatial data.

Geospatial Data and Rights Management

Distributors of data, especially geospatial data, desire control over their data's movement and use, both for their own advantage and to protect certain rights of others. The chief concerns when dealing with geospatial data are privacy, information security, and property. Privacy is defined as "an individual's claim to control the terms under which personal information – information identifiable to an individual – is acquired, disclosed, or used" (Privacy Working Group, 1995). Information security is the protection of information from unauthorized access and ensures the information's integrity. Property is the protection of the rights of the owner of data with regard to the data.

Different rights will be more important to different distributors, notably a greater importance of property in the private sector and security in the public sector. Also, control over data can protect the distributor (or provider) from liability for data, ensure regular data update to maintain quality, and ease the process of data distribution itself (Joffe, 2003).

The rights of privacy and security are usually preserved by simple limitation of access to particular data to those specifically authorized to access them, and limitation of how they can use and distribute those data. Property is more difficult to deal with because of the many legal aspects of intellectual property that must be considered, and the great variety of possible agreements among data providers, distributors, and end users (Joffe, 2003).

Such agreements would prevent actions, such as redistribution of data, that are not advantageous to providers. Parties involved in data movement and distribution must

decide what can and cannot be done to or with the data, and be certain that these terms will be followed (Joffe, 1998).

Data providers that depend on revenue from the sale of data to remain economically viable must be able to put limits on the use of their data. However, once data providers send data out to distributors and users, they no longer have any direct control over the use and movement of their data. Therefore, they must make agreements with distributors to protect their interests. To maintain relations with data providers, distributors must be able to control who can access and use data, and how they use the data.

Geospatial data pose unusual problems for the protection of property rights. A typical use of geospatial data involves extracting information from multiple data sets and integrating that information to create a new data set, thus entering gray areas of intellectual property. It is, therefore, necessary to have detailed terms and conditions for the many aspects of access, use, and dissemination to protect the providers' interests. Historically, these agreements have relied upon subjective human judgment, the goodwill of users, the threat of litigation, and the discretion of individuals involved in the distribution process.

However, as Coyle (2004) notes, "Neither copyright law nor contracts assert any actual control over the behavior of users of materials. Instead, they rely on the parties to act within the stated agreement or law." With the advent of digital methods of data distribution, the scale and ease of data movement have both increased, placing more emphasis on enforcement of these agreements, while simultaneously becoming more difficult to enforce solely through human judgment. Digital Rights Management (DRM) allows new possibilities in precise and rigorous management of data access and use.

What is Digital Rights Management?

DRM is the concept of digital enforcement of rights for the access and use of data. DRM provides an automated system that will consistently and rigorously enforce agreements made among users, providers, and distributors. It allows the distributor of data to control how and by whom data are used, in accordance with rules and agreements.

A good DRM system serves several purposes. First, it makes sure that agreements and contracts are rigorously observed. Second, it eases the process of data distribution, and works to ensure data quality and oversee any necessary financial transfers. Third, it protects the basic rights of privacy, property, and information security.

There are several main components to a DRM system. One is the data. Another component is the rights policy, which is a document attached to the data that specifies what can and cannot be done to and with them. A third component is the DRM framework, which provides for the movement of data and ensures that the rights specified by the rights policies are enforced (Iannella, 2001).

The DRM framework serves to preserve and apply rights policies to the data to which they are attached. The DRM framework must ensure that the rights policy is followed, and also ensure that the policy remains attached to the data, unchanged unless the policy itself provides for modifications.

A functional architecture of a DRM framework is split into three areas: intellectual property (IP) asset creation and capture, IP asset management, and IP asset usage. At asset creation, the provider of the asset (in this case, geospatial data) assigns a rights policy detailing what can and cannot be done with the data. In asset management, the data asset is transferred, but the provider's interests remain identified in the rights policy that accompanies the asset. In asset usage, the asset is accessed and used by the end user, in accordance with the terms of the rights policy. All of these components of the framework must be within the same system, otherwise it is impossible to ensure that the rights policy will be enforced (Iannella, 2001).

Coyle (2004) notes that, "Because digital materials must be mediated through software and hardware for use, it is possible to exercise *a priori* control over access to and use of the content through that technology." Effective controls require that the data and the software used for data management, transmission and usage remain within a unified DRM framework.

What is a Rights Expression Language?

A rights expression language (REL) is a language that provides a syntax and vocabulary for the expression of agreed-upon rights and the conditions to which those rights are subject. Every rights policy is written in a REL. RELs are designed to be machine-actionable, so they must have a precise and organized syntax. They must also have a very precise vocabulary, so as to avoid vagueness in instructions (Coyle, 2004).

To have a functional DRM system, it is necessary to have a standard REL throughout the entire framework. Different software can process the REL and apply the policies, but as long as all software involved understands the same REL, that REL is precise, and the software works correctly, the same results will always occur.

The choice of REL is integral to the design of a DRM system. The DRM framework must be able to distinguish among the types of data for which control is exercised, and the various types of control to be exercised. RELs provide an initial syntax and vocabulary for basic data types and actions. However, geospatial data have unique data types and processes for extracting and combining data. Therefore, the most important qualities of a REL for geospatial data are extensibility and flexibility to handle these unique aspects of geospatial data. Another desirable characteristic for a REL is that it be sufficiently abstract to allow for any needed extension and modification.

There are many rights expression languages. Two prominent ones are MPEG-21/5 and Open Digital Rights Language (ODRL). MPEG-21/5 is designed especially for use with media, such as video and audio recordings, and is integrated into a system of standards

for such digital resources. This gives it the great boon of being extensively implemented from the beginning.

ODRL is "a standard language and vocabulary for the expression of terms and conditions over assets. ODRL covers a core set of semantics for these purposes including the rights holders and the expression of permissible usages for asset manifestations" (Iannella, 2002). ODRL is designed to define almost any type of agreement, is independent of media or content, and is extremely abstract (Coyle, 2004).

The most important characteristics of ODRL are its flexibility and extensibility. It has no intended media type for its use, and can be modified extensively. Because it is open-source and based on the eXtensible Markup Language (XML), modification is free and simple. Another advantage of its flexibility is that it does not mandate any specific DRM software to use it; it is merely a language for expressing rights. ODRL, however, does have some disadvantages. One is that ODRL does not control access, but only usage. Therefore, another system must be used for identification and validation of users. ODRL, though not initially designed with an implementation available, has also been tested and a form of it is used in the popular OMA DRM standard.

The key element to the flexibility of ODRL is the data dictionary. This is a part of ODRL that defines data types, constraints, and many other parts of ODRL, and can be very easily added to and modified. The basic categories of the ODRL data dictionary are rights, expressed as permissions, and the limits on those rights, expressed through context, constraints, and requirements. Permissions are actions that a user is able to perform if they meet the constraints and requirements on the permission. Contexts apply not only to permissions, but also to parties involved, and merely serve to give more information about the entity with which they are associated. Constraints define things that must be true for the user to have the permission, and requirements are actions, such as payment, that a user must take to exercise the permission. The data dictionary can be easily extended or modified, to create new entities of any type within the basic ODRL syntax, which can also be modified.

Geospatial Data and ODRL

Geospatial data are a fairly specialized use for a REL, and the geospatial community may find it inefficient and too costly to develop a completely new REL specifically for geospatial data. A better choice is to find an existing REL that is sufficiently extensible, flexible, and abstract to take advantage of uses that the REL has in common with other application communities, but also to allow the expression of interests unique to the geospatial community. ODRL is a REL that meets those criteria.

As an example of the application of ODRL to geospatial data, consider a provider of Digital Orthophoto Quadrangles (DOQs). The provider wishes all of their DOQs to be available freely for viewing and aggregation to Emergency First Responders. All others will be able to view DOQs for free at a resolution of 1 (measured by an arbitrary scale

from 1 to 10), but must pay $10.00 per view at higher resolutions. Also, all will be able to aggregate these DOQs into other data by paying a one-time fee of $75.00.

The permissions to be granted are “display” and “aggregate.” The exact meanings of these terms are defined by the software that reads the rights policy. In general, display is the right to simply view the data, and aggregate is the right to use the data by integrating them into another set of data.

The first step to express this rights policy is the definition of terms within the data dictionary. If one wishes to add a way of dealing with resolutions to ODRL, the basic vocabulary of ODRL can be extended to include this concept. A new constraint named “res,” an integer with a range of 1 to 10, is declared. The resolution of the data will be contained within the data themselves, and the software checks the data’s resolution against the constraint to enforce the rights policy.

The dictionary extension begins by incorporating into itself the base ODRL data dictionary and syntax at http://odrl.net and declaring itself as existing at http://example.net as GEO-DD.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema targetNamespace="http://example.net/GEO-DD"
                        xmlns:xsd="http://www.w3.org/2001/XMLSchema"
                        xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
                        xmlns:geo="http://example.net/GEO-DD"
                        elementFormDefault="qualified"
                        attributeFormDefault="qualified">
    <xsd:import namespace="http://odrl.net/1.1/ODRL-EX"
            schemaLocation="http://odrl.net/1.1/ODRL-EX-11.xsd"/>
```

A new constraint of resolution, defined as “res,” is added to the basic ODRL vocabulary.

```
    <xsd:element name="res" type=”xsd:positiveInteger”
            substitutionGroup="o-ex:constraintElement"/>
</xsd:schema>
```

The rights policy begins by accessing the ODRL syntax and data dictionary at odrl.net and the geo data dictionary extension at http://example.net.

```
<?xml version="1.0" encoding="UTF-8"?>
<o-ex:rights xmlns:o-ex="http://odrl.net/1.1/ODRL-EX"
                        xmlns:o-dd=”http://odrl.net/1.1/ODRL-DD”
                        xmlns:geo=”http://example.net/GEO-DD”>
```

The policy begins the agreement, defining the asset (the DOQ) attached as having the unique id UNIQUEDOQ112.

```
<o-ex:agreement>
    <o-ex:asset>
        <o-ex:context>
            <o-dd:uid>UNIQUEDOQ112</o-dd:uid>
        <o-ex:context>
    </o-ex:asset>
```

The first permission granted is the right to display the asset at the resolution of 1.

```
    <o-ex:permission>
        <o-dd:display>
            <o-ex:constraint>
                <geo:res> 1 </geo:res>
            </o-ex:constraint>
        </o-dd:display>
    </o-ex:permission>
```

The second permission is to display and aggregate the asset, with no cost, if the group constraint is met by the user being in the group of Emergency First Responders (EmFiResp).

```
    <o-ex:permission>
        <o-dd:display/>
        <o-dd:aggregate/>
        <o-ex:constraint>
            <o-dd:group>
                <o-ex:context>
                    <o-dd:uid>EmFiResp</o-dd:uid>
                </o-ex:context>
            </o-dd:group>
        </o-ex:constraint>
    </o-ex:permission>
```

The third permission introduces a requirement, which is an action that must be taken to enact the permission granted. In this case, the permission is to display, and the requirement is that the user pay a fee of $10.00 U.S. Dollars (USD) per use.

```
    <o-ex:permission>
        <o-dd:display/>
        <o-ex:requirement>
            <o-dd:peruse>
                <o-dd:payment>
                    <o-dd:amount o-dd:currency=”USD”>
                        10.00
                    </o-dd:amount>
                </o-dd:payment>
            </o-dd:peruse>
```

```
            </o-ex:requirement>
        </o-ex:permission>
```

To aggregate the data, a single one-time prepayment of $75.00 USD is required.

```
        <o-ex:permission>
            <o-dd:aggregate/>
            <o-ex:requirement>
                <o-dd:prepay>
                    <o-dd:payment>
                        <o-dd:amount o-dd:currency="USD">
                            75.00
                        </o-dd:amount>
                    </o-dd:payment>
                </o-dd:prepay>
            </o-ex:requirement>
        </o-ex:permission>

    </o-ex:agreement>
    </o-ex:rights>
```

This example shows only a few of the possible rights that can be expressed using ODRL, but represents the form all expressions would take. Many more permission, constraint, and requirement types are available. As shown in the data dictionary extension above, it is very easy to define new elements of various types needed for geospatial data.

Conclusion

Geospatial Digital Rights Management is a way of ensuring that agreements made between creators, distributors, and users of geospatial data are adhered to and honored by all parties. The distributor must create a DRM system with a framework to implement the rights described in right policies, written in a REL. Because the REL is the foundation of a good DRM system, it must be carefully chosen. ODRL has the qualities of flexibility and extraction needed for geospatial data.

Bibliography

Coyle, Karen. 2004. Rights Expression Languages, A Report for the Library of Congress. Library of Congress Website at www.loc.gov/standards/relreport.pdf (accessed August 4, 2004).

Joffe, Bruce. 1998. The GIS Data Sales Dilemma: Finding a Middle Ground. Open Data Consortium Website at www.opendataconsortium.org. (accessed July 12, 2004).

Joffe, Bruce. 2003. Data Distribution Policy Issues. Open Data Consortium website at www.opendataconsortium.org. (accessed July 12, 2004).

Iannella, Renato. 2001. Digital Rights Management (DRM) Architectures, D-Lib Magazine, June 2001, 7(6).

Iannella, Renato. 2002. Open Digital Rights Language (ODRL) Version 1.1. W3C Note, 19 September 2002. W3C website at www.w3.org/TR/odrl. (accessed August 4, 2004).

Privacy Working Group, US Information Infrastructure Task Force. 1995. Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information, October 1995. U.S. Department of Health and Human Services Website at http://aspe.hhs.gov/datacncl/niiprivp.htm (accessed August 19, 2004).